CLAIMS

What is claimed is:

1. A method of evaluating fraud risk of an electronic commerce transaction, the method comprising the computer-implemented steps of:

receiving transaction information that defines the electronic commerce transaction;

determining a first fraud risk score value associated with the electronic transaction based on applying a plurality of tests to the transaction information, wherein each of the plurality of tests determines whether the transaction information appears to represent a genuine transaction based on specified criteria;

determining a second fraud risk score value associated with the electronic transaction based on a comparison of the transaction information to historical transaction information;

combining the first fraud risk score value and the second fraud risk score value using a statistical model to result in creating a model score value;

blending the model score value with one or more merchant-specific threshold values to result in creating and storing a final fraud risk score value for the transaction.

2. A method as recited in Claim 1, wherein receiving transaction information comprises the steps of receiving transaction information that defines the electronic commerce transaction for a particular Internet identity, and wherein determining a second fraud risk score value comprises the steps of determining a second fraud risk score value associated with the electronic transaction based on a comparison of the transaction information to historical transaction information for other transactions pertaining to the same Internet identity.

3. A method as recited in Claim 2, wherein an Internet identity comprises a first hash value of an email address of a prospective purchaser carried in combination with a second hash value of a card bank identification number of the prospective purchaser.

4. A method as recited in Claim 2, wherein an Internet identity comprises a first hash value of an email address of a prospective purchaser carried in combination with a second hash value of a card bank identification number of the prospective purchaser and with a third hash value based on a shipping address of the prospective purchaser.

5. A method as recited in Claim 2, wherein an Internet identity comprises a first hash value of an prospective purchaser's host IP address, in combination with a second hash value of an email address of a prospective purchaser carried, in combination with a third hash value of a card bank identification number of the prospective purchaser and a fourth hash value based on a shipping address of the prospective purchaser.

6. A method as recited in Claim 2, wherein an Internet identity comprises a first hash value of a prospective purchaser's hardware device ID value, in combination with a second hash value of either the email address or user ID of the prospective purchaser, in combination with a third hash value of a card bank identification number of the prospective purchaser and with a fourth hash value based on a shipping address of the prospective purchaser.

7. A method as recited in Claim 1, wherein the step of determining the second fraud risk score value comprises the steps of:

retrieving one or more records of historic transaction information pertaining to past transactions associated with the transaction information;

when one of the records of historic transaction information is found to contain a fraud list tag, discontinuing further retrieval of such records;

determining a second fraud risk score value associated with the electronic transaction based on only the retrieved records of historical transaction information in comparison to the transaction information.

8. A method as recited in Claim 1, wherein the step of determining the second fraud risk score value comprises the steps of:

retrieving one or more records of historic transaction information pertaining to past transactions associated with the transaction information;

when a specified large plurality of the records of historic transaction information is retrieved and further records of historic transaction information remain to be retrieved, discontinuing further retrieval of such records;

determining a second fraud risk score value associated with the electronic transaction based on only the retrieved records of historical transaction information in comparison to the transaction information.

9. The method as recited in Claim 1, wherein the step of blending the model score value comprises the steps of blending the model score value with one or more merchant-specific threshold values to result in creating and storing a final fraud risk score value for the transaction and one or more return code values that signal specified risk issues that have been detected with respect to the transaction.

10. The method as recited in Claim 1, wherein determining the first fraud risk score value comprises the steps of determining a first fraud risk score value associated with the electronic transaction based on applying a plurality of tests to the transaction information, wherein one of the plurality of tests determines whether an Internet identity in the transaction information is found in a list of parties to known past fraudulent transactions.

11. The method as recited in Claim 1, wherein determining the first fraud risk score value comprises the steps of determining a first fraud risk score value associated with the electronic transaction based on applying a plurality of tests to the transaction information, wherein one of the plurality of tests determines whether an Internet identity in the transaction information is found in a list of trusted parties.

12. A method as recited in Claim 1, wherein determining the first fraud risk score value comprises the steps of determining a first fraud risk score value associated with the electronic transaction based on applying a plurality of tests to the transaction information, wherein one of the plurality of tests automatically determines whether a text value in the transaction information is unintelligible or meaningless, by the steps of:

receiving the text value;

for each bi-gram in the text value, retrieving from a table of bi-gram probability values a probability value that represents a probability that the bi-gram is found in a genuine text value;

generating a penalty value when the retrieved probability values indicate that the text value comprises a combination of bi-grams that are not likely to represent a genuine text value.

13. A method as recited in Claim 1, wherein determining the first fraud risk score value comprises the steps of determining a first fraud risk score value associated with the electronic transaction based on applying a plurality of tests to the transaction information, wherein one of the plurality of tests automatically determines whether a name value in the transaction information is unintelligible or meaningless, by the steps of:

receiving the name value;

for each bi-gram in the text value, retrieving from a table of bi-gram probability values a probability value that represents a probability that the bi-gram is found in a genuine name value, wherein the table of bi-gram probability values is created based on an actual frequency of occurrences of bi-grams in a large sample of genuine names;

generating a penalty value when the retrieved probability values indicate that the text value comprises a combination of bi-grams that are not likely to represent a genuine name value.

14. A method as recited in Claim 1, wherein determining the first fraud risk score value comprises the steps of determining a first fraud risk score value associated with the electronic transaction based on applying a plurality of tests to the transaction information, wherein one of the plurality of tests automatically determines whether a city value in the transaction information is within an area code value of the transaction information, by the steps of:

receiving the city value and the area code value as part of transaction information;

determining a latitude value and a longitude value that represent a true position of a city identified in the city value;

determining a range of latitude values and a range of longitude values associated with an area code identified in the area code value;

based on the latitude values and longitude values, determining whether the city identified in the city value is genuinely within the area code identified in the area code value;

applying a penalty to the transaction when the city identified in the city value is not within the area code identified in the area code value.

15. A method as recited in Claim 1, wherein determining the first fraud risk score value comprises the steps of determining a first fraud risk score value associated with the electronic transaction based on applying a plurality of tests to the transaction information, wherein one of the plurality of tests automatically determines whether a city value in the transaction information is within an email domain of the transaction information, by the steps of:

receiving the city value and an email address value as part of transaction information;

determining a latitude value and a longitude value that represent a true position of a city identified in the city value;

determining a range of latitude values and a range of longitude values associated with an email domain portion of the email address value;

based on the latitude values and longitude values, determining whether the city identified in the city value is genuinely within the email domain indicated in the email address value;

applying a penalty to the transaction when the city identified in the city value is not within the area code identified in the area code value.

16. A method as recited in Claim 13, further comprising the steps of creating and storing an email domain location table comprising a plurality of records that associate email domain values with city values associated with shipping addresses of past non-fraudulent transactions.

17. The method as recited in Claim 14, wherein determining whether the city identified in the city value is genuinely within the email domain comprises the steps of determining whether the city value is for a city that is outside the email domain as indicated by the records in the email domain location table.

18. A method as recited in Claim 1, wherein determining the first fraud risk score value comprises the steps of determining a first fraud risk score value associated with the electronic transaction based on applying a plurality of tests to the transaction information, wherein one of the plurality of tests automatically determines whether a country value in the transaction information is proximate to a bank referenced in a bank identification number of a credit card number in the transaction information, by the steps of:

receiving the country value and a bank identification number of a credit card number as part of transaction information;

determining a relative distance between a country identified in the country value and a bank associated with the bank identification number;

based on the relative distance between the country and the bank, determining whether the country is too far from the bank;

applying a penalty to the transaction when the country is too far from the bank.

19. A method as recited in Claim 18, further comprising the steps of creating and storing a bank location table comprising a plurality of records, wherein each record associates a bank identification number with a country value representing a country in which a headquarters of the bank is located.

20. A method as recited in Claim 19, further comprising the steps of creating and storing a bank location table comprising a plurality of records that associate bank identification numbers with country values associated with shipping addresses of past non-fraudulent transactions.

21. The method as recited in Claim 20, wherein determining whether the country identified in the country value is too far from the bank comprises the steps of determining whether the country value is for a country that is too far from the bank as indicated by the records in the bank domain location table.

22. A method of determining evaluating fraud risk of an electronic commerce transaction, the method comprising the computer-implemented steps of:
receiving transaction information that defines the electronic commerce transaction;
determining a first fraud risk score value associated with the electronic transaction
based on applying a plurality of tests to the transaction information, wherein one of the plurality of tests automatically determines whether a name value in the transaction information is unintelligible or meaningless, by:
receiving the name value;
for each bi-gram in the text value, retrieving from a table of bi-gram probability values a probability value that represents a probability that the bi-gram is found in a genuine name value, wherein the table of bi-gram probability values is created based on an actual frequency of occurrences of bi-grams in a large sample of genuine names;

generating a penalty value when the retrieved probability values indicate that the text value comprises a combination of bi-grams that are not likely to represent a genuine name value.

23. A method of determining for an electronic commerce transaction whether a text value is gibberish, comprising the steps of:

receiving the text value as part of transaction information of the electronic commerce transaction;

identifying a succession of letter pairs in the received text value;

for each identified letter pair, retrieving from a table of probability values a probability value that represents a probability that the identified letter pair is found in a genuine text value in a position equivalent to a position of each identified letter pair within the received text value;

generating a fraud risk penalty value for the electronic commerce transaction when the retrieved probability values indicate that the received text value is not likely to represent a genuine text value.

24. A computer-readable medium carrying one or more sequences of instructions for evaluating fraud risk of an electronic commerce transaction, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

receiving transaction information that defines the electronic commerce transaction;

determining a first fraud risk score value associated with the electronic transaction based on applying a plurality of tests to the transaction information, wherein each of the plurality of tests determines whether the transaction information appears to represent a genuine transaction based on specified criteria;

determining a second fraud risk score value associated with the electronic transaction based on a comparison of the transaction information to historical transaction information;

combining the first fraud risk score value and the second fraud risk score value using a statistical model to result in creating a model score value;

blending the model score value with one or more merchant-specific threshold values to result in creating and storing a final fraud risk score value for the transaction.

25. An apparatus for evaluating fraud risk of an electronic commerce transaction, comprising:

means for receiving transaction information that defines the electronic commerce transaction;

means for determining a first fraud risk score value associated with the electronic transaction based on applying a plurality of tests to the transaction information, wherein each of the plurality of tests determines whether the transaction information appears to represent a genuine transaction based on specified criteria;

means for determining a second fraud risk score value associated with the electronic transaction based on a comparison of the transaction information to historical transaction information;

means for combining the first fraud risk score value and the second fraud risk score value using a statistical model to result in creating a model score value;

means for blending the model score value with one or more merchant-specific threshold values to result in creating and storing a final fraud risk score value for the transaction.

26. An apparatus for evaluating fraud risk of an electronic commerce transaction, comprising:

a processor;

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

receiving transaction information that defines the electronic commerce transaction;

determining a first fraud risk score value associated with the electronic transaction based on applying a plurality of tests to the transaction information, wherein each of the plurality of tests determines whether the transaction information appears to represent a genuine transaction based on specified criteria;

determining a second fraud risk score value associated with the electronic transaction based on a comparison of the transaction information to historical transaction information;

combining the first fraud risk score value and the second fraud risk score value using a statistical model to result in creating a model score value;

blending the model score value with one or more merchant-specific threshold values to result in creating and storing a final fraud risk score value for the transaction